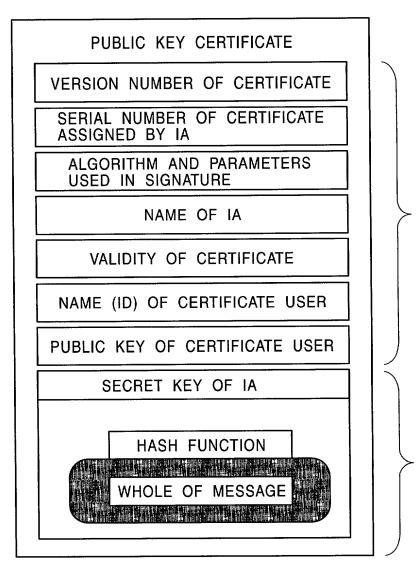
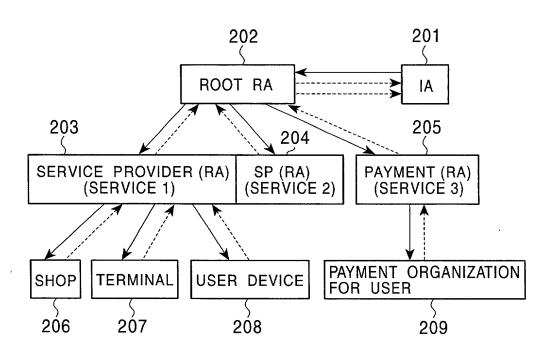
FIG. 1



WHOLE OF MESSAGE

ELECTRONIC SIGNATURE

FIG. 2



AUTHENTICATED ← AUTHENTICATING PARTY

-----> : FLOW OF REGISTRATION

FIG. 3

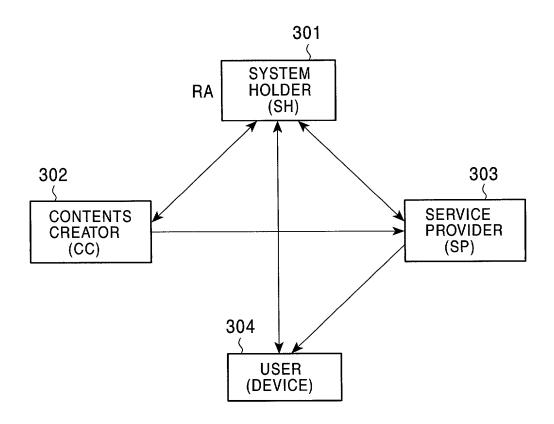


FIG. 4

NO.	SYSTEM HOLDER (SH)	CONTENTS CREATOR (CC)	SERVICE PROVIDER (SP)	USER DEVICE
-	INTERNET SHOPPING MARKET SPONSOR	MARKETED GOODS PRODUCER AND CONTENTS CREATOR	MARKETED GOODS SHOP	PC
2.	CELLULAR PHONE COMMUNICATION INFRASTRUCTURE PROVIDER	PRODUCER OF CONTENTS AND GOODS PROVIDED USING CELLULAR PHONE INFRASTRUCTURE	CONTENTS DELIVERER TO CELLULAR PHONE USER	CELLULAR PHONE
_. ه	CABLE-TV CABLE MANAGING ORGANIZATION	CABLE TV PROGRM PRODUCER	CABLE TV COMPANY	TV (SET)
4	ELECTRONIC MONEY CARD ISSUER	PRODUCER OF CONTENTS AND GOODS PURCHASABLE WITH ELECTRONIC MONEY	ELECTRONIC MONEY AVAILABLE SHOP	IC CARD
5.			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
6.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

525 521 IA-B USER (DEVICE) 522 CA-B SERVICE B RA-B SERVICE PROVIDER (SP) EXAMING AUTHORITY 524 523 520 FIG. 5 511 IA-A USER (DEVICE) 512 CA-A 515 SERVICE A RA-A SERVICE PROVIDER (SP) EXAMING AUTHORITY 513 514 510

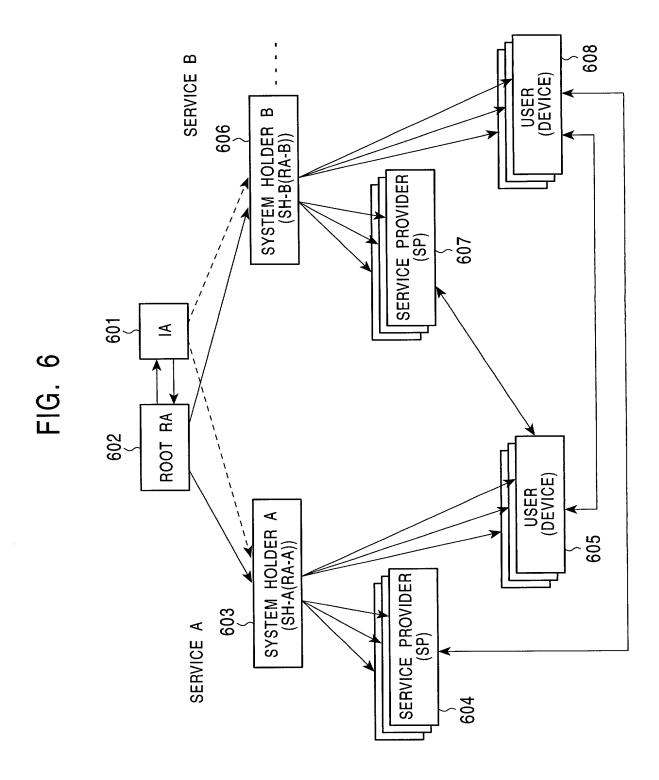
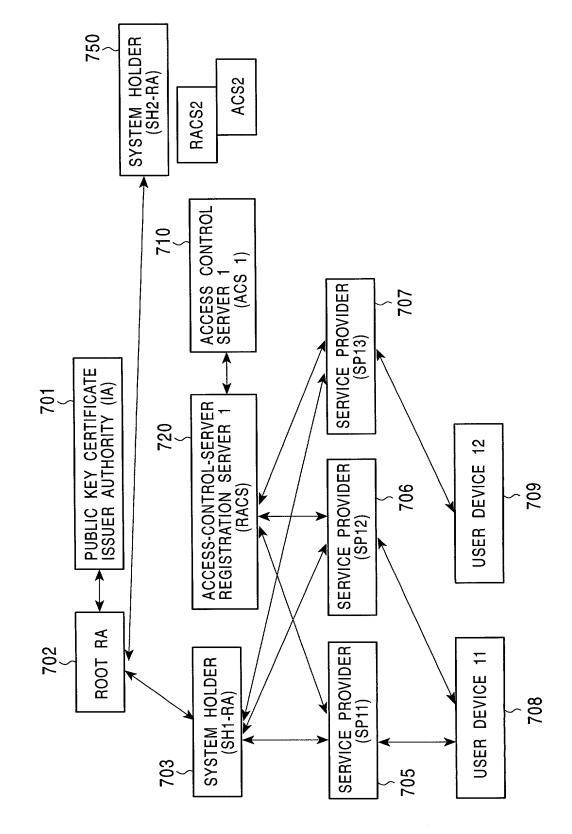


FIG. 7



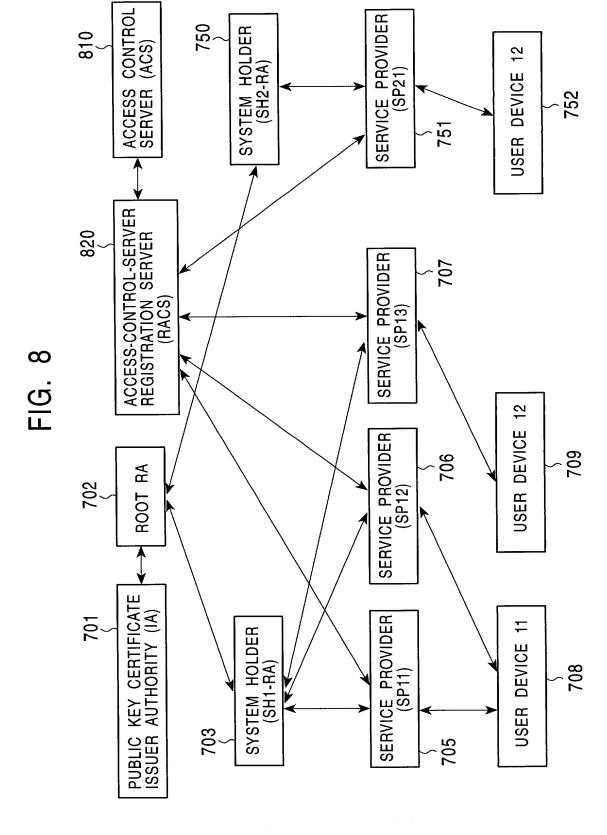
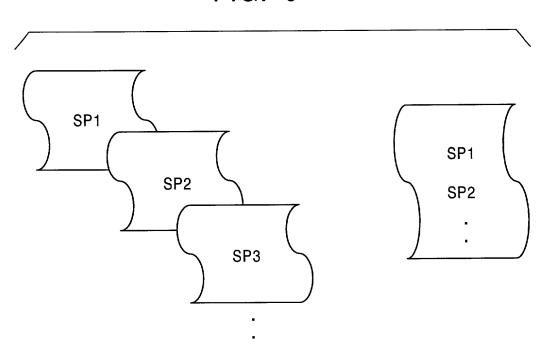


FIG. 9



METHOD A

METHOD B

FIG. 10

		SERIAL NUMBER
FIVED FIELD		VALIDITY
FIXED FIELD	SERIA	L NUMBER OF PUBLIC KEY CERTIFICATE (PKC)
SET BY ACCESS CONTROL SERVER		VERSION NUMBER
(ACS)		ISSUER ID
		SIGNATURE ALGORITHM
		OPTION FIELD SIZE
	SP1	SERVICE PROVIDER (SP) ID
OPTION FIELD		DATA SIZE
<u> </u>		CONTENTS (SEE FIG. 11)
SET BY EACH SERVICE	SP2	SERVICE PROVIDER (SP) ID
PROVIDER (SP)		DATA SIZE
		CONTENTS (SEE FIG. 11)
		•
SIGNATURE FIELD (ACS)		SIGNATURE

FIG. 11

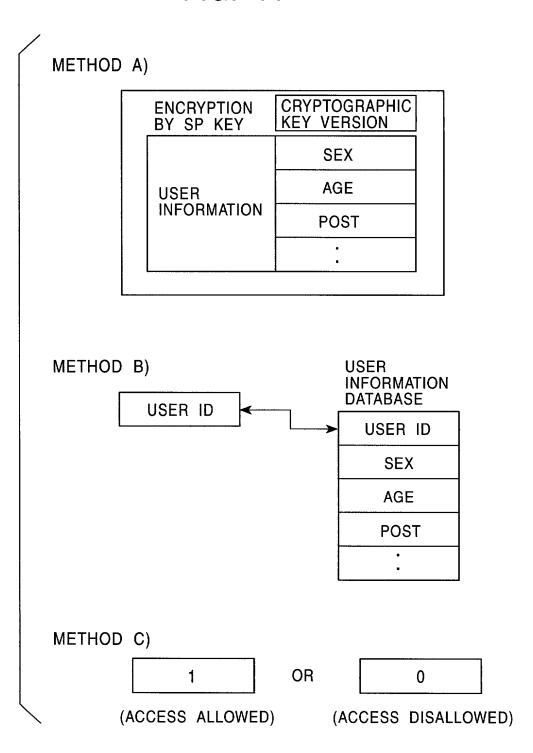


FIG. 12

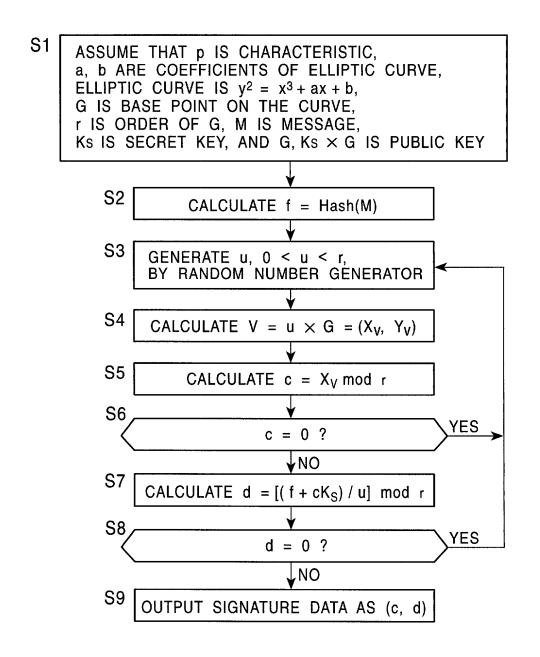


FIG. 13

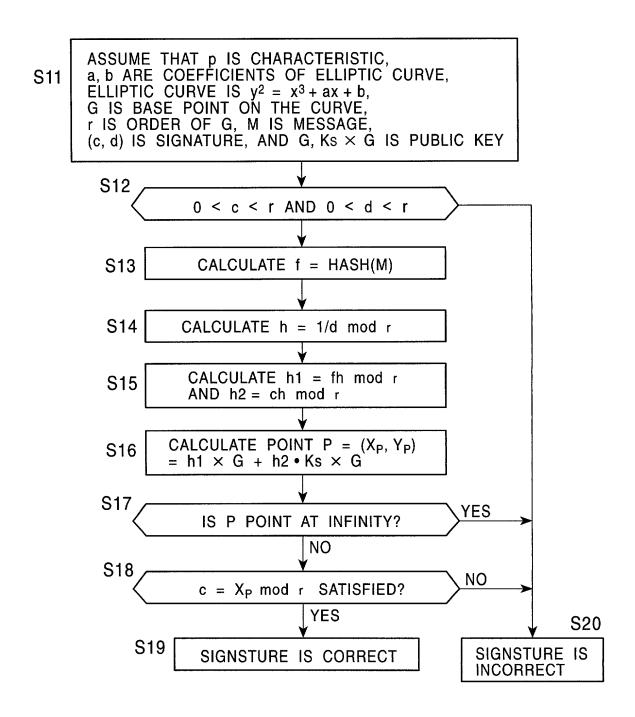


FIG. 14

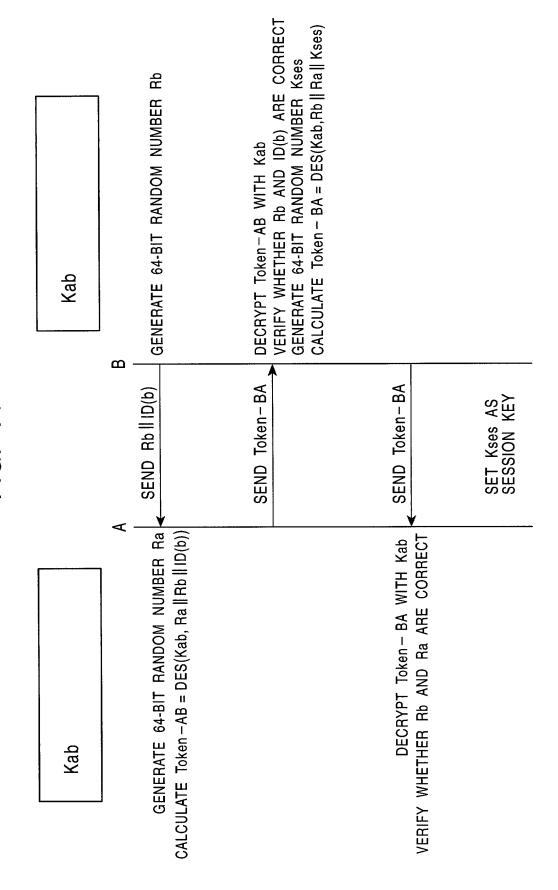


FIG. 15

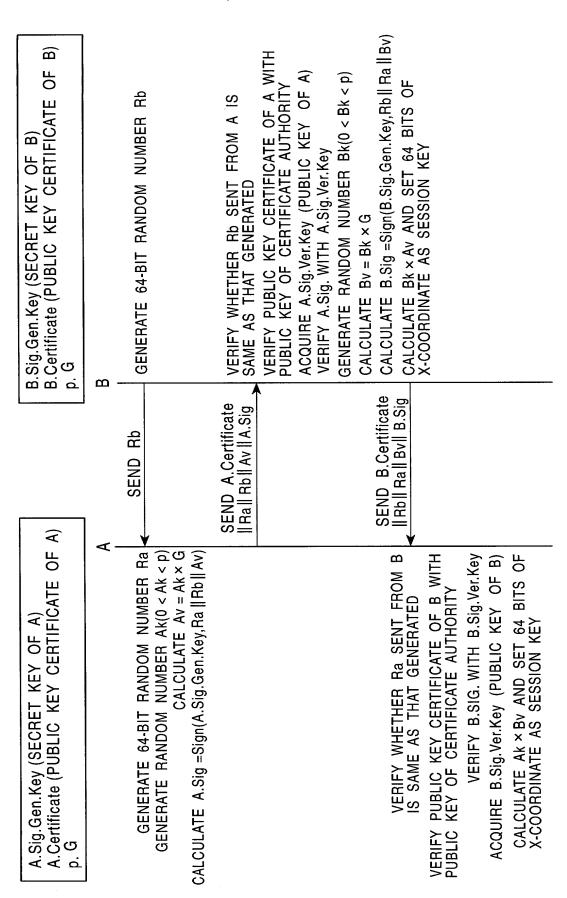


FIG. 16

Š.	TERM	SYMBOL	DESCRIPTION / REMARKS
-	PUBLIC KEY	Кра	PUBLIC KEY OF A
		s -	EXAMPLE User → KPa UD → KPud SP → KPsp
2	SECRET KEY	Ksa	SECRET KEY OF A
		3	EXAMPLE User → Ksu UD → Ksud SP → Ksp
က	SESSION KEY	Ks	COMMON KEY CREATED IN MUTUAL AUTHENTICATION
4	CERTIFICATE	A «B»	CERTIFICATE OF B ISSUED BY A EXAMPLE: CERTIFICATE OF UD ISSUED BY IA → IA≪UD≫
5	ENCRYPTION	E _{Ks} (data)	ENCRYPT PLAINTEXT DATA WITH KEY Ks
9	DECRYPTION	D _{Ks} (data)	DECRYPT CIPHERTEXT DATA WITH KEY KS
7	SIGNATURE	{data}Sig.K _{Sa}	PUT SIGNATURE TO DATA WITH SECRET KEY KSa OF A
ω	ENCRYPTION WITH SIGNATURE	E _{Ka} ({data}Sig.K _{Sa})	PUT SIGNATURE TO DATA WITH SECRET KEY K _{Sa} OF A AND ENCRYPT (DATA SIGNATURE) WITH KEY K _S

FIG. 17

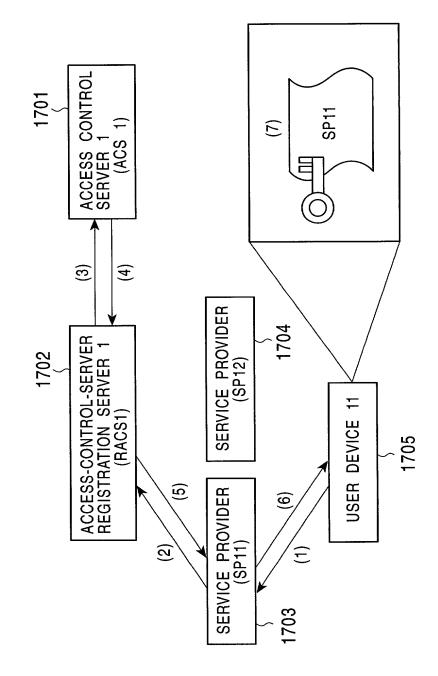


FIG. 18

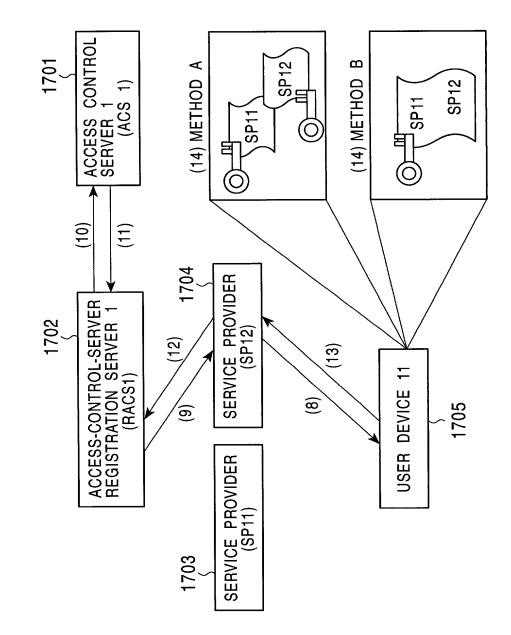


FIG. 19

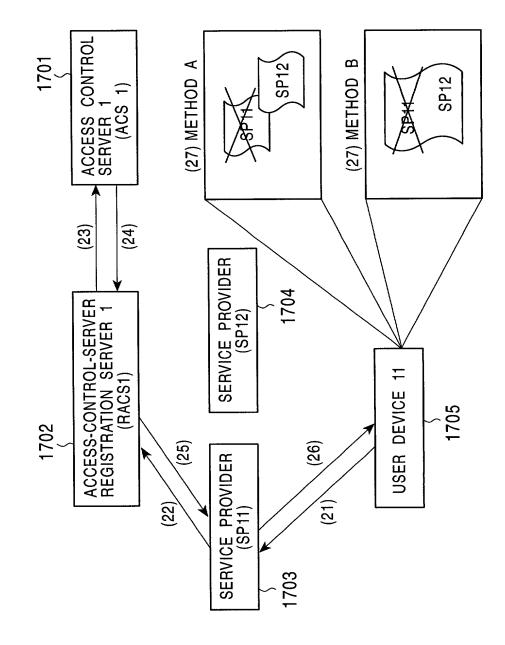


FIG. 20

٠.

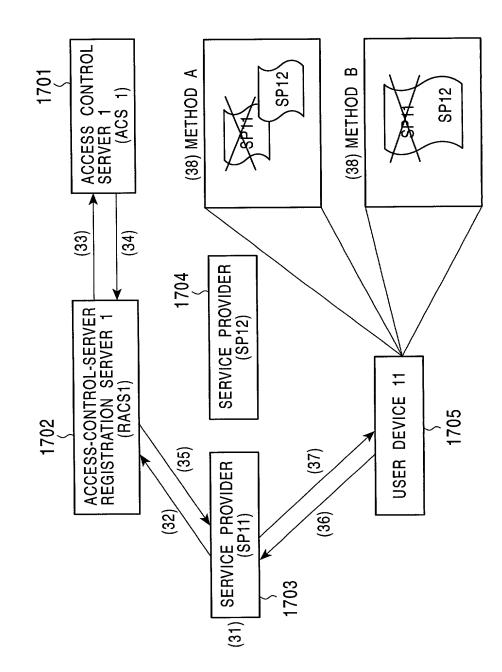


FIG. 21

1,

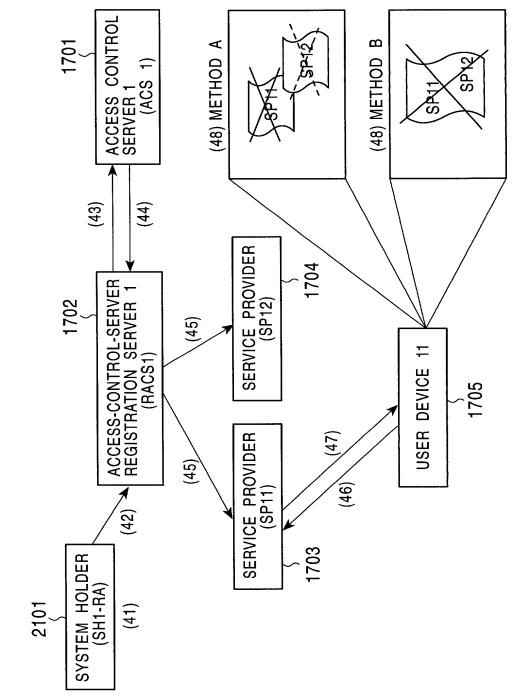
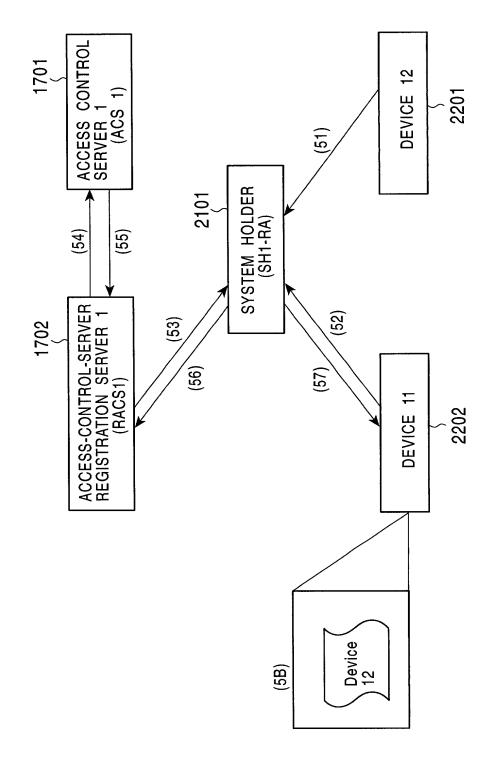


FIG. 22



3121

-3122

٠,



REMOVABLE STORAGE MEDIUM MEMORY (SECURE MODULE) 3106 CRYPTOGRAPHIC PROCESSING MEANS 3105 3114 DRIVE INPUT / OUTPUT INTERFACE COMMUNICA-TING UNIT 3113 FIG. 23 3104 HDD BUS 3103 RAM OUTPUT UNIT 3112 3102 ROM 3111 INPUT 3101 CPU

REMOVABLE STORAGE MEDIUM CRYPTOGRAPHIC PROCESSING MEANS 4114 4105 4113 DRIVE 4103 FIG. 24 RAM COMMUNICA-TING UNIT 4112 4102 ROM COMMUNICA-TING UNIT 4111 SPU

τ ,